



# **VIRGINIA COMMONWEALTH UNIVERSITY**

## **REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2013**

## **AUDIT SUMMARY**

We have audited the basic financial statements of Virginia Commonwealth University as of and for the year ended June 30, 2013, and issued our report thereon, dated October 31, 2013. Our report, included in Virginia Commonwealth University's basic financial statements, is available at the Auditor of Public Accounts' website at [www.apa.virginia.gov](http://www.apa.virginia.gov) and at Virginia Commonwealth University's website at [www.vcu.edu](http://www.vcu.edu).

Our audit of Virginia Commonwealth University for the year ended June 30, 2013, found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring Management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance or other matters required to be reported under Government Auditing Standards.

-TABLE OF CONTENTS-

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-2
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	3-4
UNIVERSITY RESPONSE	5-9
UNIVERSITY OFFICIALS	10

## INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

### **Improve Change Management**

Virginia Commonwealth University (VCU) allows IT staff with privileged system user accounts to make changes to infrastructure devices that protect and support VCU's mission critical ERP system, Banner, without management approval. Without proper acknowledgement and approval, there is a higher risk of changes negatively affecting the environment and the layers of security established to protect data in the Banner system.

We recommend that VCU amend its change management policy to ensure that all changes require management approval. Proper change management will help maintain confidentiality, integrity, and availability over VCU's critical systems and infrastructure.

### **Improve Firewall Management**

VCU does not manage its firewall that supports its Banner ERP system and safeguards sensitive information in accordance with the Commonwealth's information security standard and industry best practices.

Our review noted two areas of weakness that we have communicated in detail to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls.

We recommend that VCU implement the controls discussed in our recommendation in accordance with the current Commonwealth Information Security Standard and industry best practices, such as those published by the Center for Internet Security.

### **Review System Access for Human Resources and Payroll Employees**

VCU does not perform reviews of Banner ERP system access for employees within the Human Resources and Payroll Departments. These employees have access to both personally identifiable information and payroll information, which are both intrinsically sensitive. Without regular reviews of system access there is an increased risk of fraudulent behavior within the University due to a lack of established controls ensuring appropriate segregation of duties.

During our review it was determined that employee access is only reviewed during the original role granting process, and that no reviews are performed on a regular and ongoing basis. The Commonwealth Security Standard, SEC 501-07, requires that the controls for account management must include "reviewing accounts and privileges at least annually." Additionally, to ensure appropriate segregation of duties controls are maintained, VCU's 'Banner HR Security Access Process' requires ongoing reviews of employee system access for those that have access to sensitive data.

We recommend that VCU dedicate the necessary resources to implement regular Banner access reviews that are in line with both the Commonwealth Information Security Standard and the Banner HR Security Access Process.

### **Improve Capital Asset Inventory Procedures**

For a portion of our audit involving tests of internal controls over fixed assets, we relied on work performed by VCU's Department of Assurance Services. The work performed by Assurance Services identified

that VCU's annual fixed asset inventory process failed to identify several assets that were lost, stolen, surplus, or otherwise disposed.

This finding has been previously communicated to the Board of Visitors in Assurance Services' report dated April 12, 2013. We have referenced the finding communicated by Assurance Services as the underlying work supports the financial statement audit and relates directly to certain financial statement balances. A corrective action plan has been approved and implementation is currently in process.



# Commonwealth of Virginia

## Auditor of Public Accounts

Martha S. Mavredes, CPA  
Auditor of Public Accounts

P.O. Box 1295  
Richmond, Virginia 23218

October 31, 2013

The Honorable Robert F. McDonnell  
Governor of Virginia

The Honorable John M. O'Bannon, III  
Chairman, Joint Legislative Audit  
and Review Commission

Board of Visitors  
Virginia Commonwealth University

### INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of **Virginia Commonwealth University** as of and for the year ended June 30, 2013, and the related notes to the financial statements, which collectively comprise Virginia Commonwealth University's basic financial statements and have issued our report thereon dated October 31, 2013. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of Virginia Commonwealth University, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

#### Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered Virginia Commonwealth University's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of Virginia Commonwealth University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of Virginia Commonwealth University's internal control over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified. We did identify certain deficiencies in internal control over financial reporting entitled “Improve Change Management,” “Improve Firewall Management,” “Review System Access for Human Resources and Payroll Employees,” and “Improve Capital Asset Inventory Procedures,” which are described in the section titled “Internal Control and Compliance Findings and Recommendations,” that we consider to be significant deficiencies.

#### Compliance and Other Matters

As part of obtaining reasonable assurance about whether Virginia Commonwealth University’s financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled “Internal Control and Compliance Findings and Recommendations,” in the findings entitled “Improve Firewall Management” and “Review System Access for Human Resources and Payroll Employees.”

#### Virginia Commonwealth University’s Response to Findings

We discussed this report with management at an exit conference held on October 30, 2013. Virginia Commonwealth University’s response to the findings identified in our audit is described in the accompanying section titled “University Response.” Virginia Commonwealth University’s response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

#### Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity’s internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Audit Standards in considering the entity’s internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

AUDITOR OF PUBLIC ACCOUNTS

EMS/alh



Monroe Park Campus

V i r g i n i a C o m m o n w e a l t h U n i v e r s i t y

**Finance and  
Administration**  
Office of the Vice President

October 31, 2013

McAdams House  
914 West Franklin Street  
P.O. Box 843076  
Richmond, Virginia 23284-3076

804 828-6116  
Fax: 804 828-0978  
TDD: 1-800-828-1120  
[www.finance.vcu.edu](http://www.finance.vcu.edu)

David A. Von Moll  
State Comptroller  
Virginia Department of Accounts  
P.O. Box 1971  
Richmond, VA 23218

Subject: Response to Internal Control and Compliance Findings and Recommendations  
of the Auditor of Public Accounts

Dear Mr. Von Moll:

In compliance with the Commonwealth Accounting Policies and Procedures (CAPP) Manual, Section 10200, Financial Management, Virginia Commonwealth University (VCU) is submitting its response to the "Internal Control Findings and Recommendations" of the Auditor of Public Accounts' Report on Audit for the Year Ended June 30, 2013.

Should you have any questions or require additional information, please contact me at 828-6116.

Sincerely,

William R. Decatur  
Vice President for Finance and Administration

Enclosure

cc: The Honorable Laura W. Fornash  
Martha S. Mavredes, Auditor of Public Accounts  
Daniel S. Timberlake, Department of Planning and Budget

During Virginia Commonwealth University's (VCU) annual audit, the Auditor of Public Accounts routinely considers internal controls to determine financial statement auditing procedures. Although the Auditor provides no assurance about internal controls, four reportable conditions are noted in his report.

The following internal control and compliance recommendations are included in the VCU Report on Audit for the year ended June 30, 2013:

1. Improve Change Management
2. Improve Firewall Management
3. Review System Access for Human Resources and Payroll Employees
4. Improve Capital Asset Inventory Procedures

Although the Auditor's findings indicate conditions requiring management's attention, the conditions do not have a material effect on the financial statements.

Findings of the Auditor:

1. Improve Change Management

Virginia Commonwealth University (VCU) allows IT staff with privileged system user accounts to make changes to infrastructure devices that protect and support VCU's mission critical ERP system, Banner, without management approval. Without proper acknowledgement and approval, there is a higher risk of changes negatively affecting the environment and the layers of security established to protect data in the Banner system.

We recommend that VCU amend its change management policy to ensure that all changes require management approval. Proper change management will help maintain confidentiality, integrity, and availability over VCU's critical systems and infrastructure.

VCU Response:

The VCU Change Management system is a system developed in house that allows the documentation, notification and approval of major system changes. Until recently, during certain times of the year, the Change Management system had been configured to allow a change to be entered into the system without any approval from supervisors. However, this option was disabled during critical time periods such as final exam and student registration.

There have been some compensating controls in the form of provisioning procedures and pre-provisioning security review in place to prevent certain network and system changes without proper security review and approval. However, VCU concurs with the finding and recognizes the weakness in its Change Management System that had allowed certain changes without other compensating controls to be implemented without approval. VCU concurs with the recommendation and has re-evaluated its change management policies and implemented additional controls to ensure that all changes are approved by the appropriate level of management personnel.

2. Improve Firewall Management

VCU does not manage its firewall that supports its Banner ERP system and safeguards sensitive information in accordance with the Commonwealth's information security standard and industry best practices.

Our review noted two areas of weakness that we have communicated in detail to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls.

We recommend that VCU implement the controls discussed in our recommendation in accordance with the current Commonwealth Information Security Standard and industry best practices, such as those published by the Center for Internet Security.

VCU Response:

While VCU regularly scans its centrally managed servers and promptly remediates vulnerabilities on these devices, the network equipment including the firewalls is not traditionally in scope of these scans. Further, a consistent patching process was not established for network equipment in the past. However, the network equipment is placed in a concealed network segment, where administrative access to the equipment is limited to only the network engineering staff using specific internal networks. The network equipment can neither be directly accessed from the external networks nor from a majority of the internal networks. Therefore, the limited exposure of administrative interfaces of the network equipment is a compensating control that significantly lowers the risk of compromise or unauthorized access.

Nevertheless, VCU concurs with the findings from APA. To further strengthen the security of these devices, VCU will establish a scanning process to identify vulnerabilities in the network equipment, and implement a risk based patching processes for the network equipment based on the scanning results.

3. Review System Access for Human Resources and Payroll Employees

VCU does not perform reviews of Banner ERP system access for employees within the Human Resources and Payroll Departments. These employees have access to both personally identifiable information and payroll information, which are both intrinsically sensitive. Without regular reviews of system access there is an increased risk of fraudulent behavior within the University due to a lack of established controls ensuring appropriate segregation of duties.

During our review it was determined that employee access is only reviewed during the original role granting process, and that no reviews are performed on a regular and ongoing basis. The Commonwealth Security Standard, SEC 501-07, requires that the controls for account management must include "reviewing accounts and privileges at least annually." Additionally, to ensure appropriate segregation of duties controls are maintained, VCU's 'Banner HR Security Access Process' requires ongoing reviews of employee system access for those that have access to sensitive data.

We recommend that VCU dedicate the necessary resources to implement regular Banner access reviews that are in line with both the Commonwealth Information Security Standard and the Banner HR Security Access Process.

VCU Response:

We agree with the finding and will amend the procedure that grants and verifies access to the Banner Human Resources module for VCU departmental employees to include the Human Resources and Payroll employees. We are currently implementing the following procedures:

The Director of Technical Services and Process Improvement, Director of Payroll Services, Manager of Benefits, Research and Development, Human Resources Operations Manager and Director of HR Services and Compensation and Compliance will review an employee access report immediately for their respective employees, revise access if required and report the information directly to the Assistant Vice President of Human Resources.

The employee access report will be reviewed at the beginning of each fiscal year and any issues will be addressed immediately and then reported to the Assistant Vice President of Human Resources.

Requests for access for new employees or changes in an employee's access will be reviewed by the employee's director or supervisor to ensure that the employee does not have maintenance access to forms that would allow an individual to edit an employee's record for both payroll and job change purposes. Any exceptions must be approved by the Assistant Vice President of Human Resources with official documentation retained in the department.

4. Improve Capital Asset Inventory Procedures

For a portion of our audit involving tests of internal controls over fixed assets, we relied on work performed by VCU's Department of Assurance Services. The work performed by Assurance Services identified that VCU's annual fixed asset inventory process failed to identify several assets that were lost, stolen, surplus, or otherwise disposed.

This finding has been previously communicated to the Board of Visitors in Assurance Services' report dated April 12, 2013. We have referenced the finding communicated by Assurance Services as the underlying work supports the financial statement audit and relates directly to certain financial statement balances. A corrective action plan has been approved and implementation is currently in process.

VCU Response:

The VCU Controller's Office has purchased bar code scanner software and equipment that will allow the departmental administrators to scan the inventory and compare that to the records in Banner Finance. This will provide a much more efficient process for the departments and allow them to conduct the inventories with minimal resources. This process, which will be used starting in FY14, will also provide the Controller's Office with hard evidence that the inventories were actually conducted and compared to Banner Finance.

VIRGINIA COMMONWEALTH UNIVERSITY  
Richmond, Virginia  
As of June 30, 2013

BOARD OF VISITORS

John C. Doswell II, Rector

William M. Ginther, Vice Rector

Jacquelyn E. Stone, Secretary

Teresa H. Carlson

Lillian L. Lambert

Kamlesh N. Dave

John A. Luke Jr.

Thomas F. Farrell II

Alexander B. McMurtie Jr.

Michael D. Fraizer

W. Baxter Perkinson, Jr.

Robert D. Holsworth

William A. Royall Jr.

Kay Coles James

Sudhakar V. Shenoy

Stuart C. Siegel

UNIVERSITY OFFICIALS

Michael Rao, President

Beverly J. Warren, Provost and Vice President for Academic Affairs

David W. Hanson, Vice President and Chief Operating Officer

Sheldon M. Retchin, Vice President for Health Services and Chief Executive Officer of the VCU Health System

Thomas C. Burke, Interim Vice President for Development and Alumni Relations

Frank L. Macrina, Vice President for Research

Wanda S. Mitchell, Vice President for Inclusive Excellence

Pamela A. Currey, Interim Vice President of Finance and Administration